

PATENT APPLICATION 10/026,403
ATTORNEY DOCKET: 72167 000570

RECEIVED
CENTRAL FAX CENTER

FEB 20 2007

THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of claims:

1. (previously presented) A method for validating credentials comprising:
inputting, at a first system that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first system;
determining, at the first system that a client does not have a valid session credential granted by the first system;
retrieving, at the first system, information from a session token held by the client, the information being retrieved from the client, the information corresponding to a session credential for the second system, the second system (1) grants session credentials based on successful authentication at the second system, and (2) includes a protected resource on the second system that is accessible by the client;
the first system presenting at least some of the information from the session token to the second system;
the first system inputting a determination from the second system that the client has a valid session credential with the second system; and
the first system granting access, to the protected resource on the first system, to the client based on the determination from the second system that the client has a valid session credential with the second system.

2. (previously presented) A method according to claim 1, further comprising

granting a session credential to the client by the first system, after determining that the client has a valid session credential granted by the second system.

3. (previously presented) A method according to claim 1, further comprising sending a session token to the client, the token corresponding to a session credential granted by the first system.

4. (previously presented) A method according to claim 1, further comprising directing the client to the second system to establish a session credential based on successful authentication at the second system, after determining that the client does not have a valid session credential granted by the second system.

5. (previously presented) A method according to claim 1, further comprising directing the client to the first system to establish a session credential based on successful authentication at the first system, after determining that the client does not have a valid session credential granted by the second system.

6. (previously presented) A method according to claim 1, further comprising maintaining the client session credential granted by the second system.

7. (Canceled)

8. (original) A method according to claim 1, wherein retrieving information from the session token held by the client comprises:

sending a query to the client from the first system, the query including identification as originating from a domain name corresponding to the second system; and receiving a response to the query.

9. (previously presented) A method for validating session credentials of a

client comprising:

inputting, at a first system that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first system;

determining, at the first system that a client does not have a valid session credential granted by the first system;

retrieving, at the first system, information from a session token held by the client, the information being retrieved from the client, the information corresponding to a session credential for the second system that grants session credentials based on successful authentication at the second system, and the second system including a protected resource that is accessible by the client, the retrieving information from the session token held by the client comprises receiving a session token from the client corresponding to the second system;

presenting at least some of the information from the session token to the second system;

determining whether the client has a valid session credential granted by the second system, the determining whether the client has a valid session credential granted by the second system is at least partially from presenting information from the session token;

the first system inputting a determination from the second system that the client has a valid session credential with the second system; granting a session credential to the client on the first system, after determining that the client has a valid session credential granted by the second system;

sending a session token to the client, the session token corresponding to the session credential granted by the first system, the session token allowing the client access to

protected resources on the first system; and

maintaining the client session credential..

10. (previously presented) Computer executable software code stored on a computer-readable medium and transmitted as an information signal, the code for validating credentials, the code comprising:

code to input, at a first system that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first system;

code to determine, at the first system, that a client does not have a valid session credential granted by the first system;

code to retrieve, at the first system, information from a session token held by the client, the information corresponding to a session credential for the second system that grants session credentials based on successful authentication at the second system, the second system including a protected resource that is accessible by the client;

code to present at least some of the information from the session token to the second system; and

code to input, from the second system to the first system, a determination whether the client has a valid session credential granted by the second system; and

code to grant access to the protected resource on the first system, to the client based on the determination from the second system that the client has a valid session credential with the second system.

11. (previously presented) A computer readable medium having computer executable code stored thereon, the code for validating credentials, the code comprising:

code to input, at a first system that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first system;

code to determine, at the first system that the client does not have a valid session credential granted by the first system;

code to retrieve from the client, at the first system, information from a session token held by the client, the information corresponding to a possible session credential for the second system that grants session credentials based on successful authentication at the second system and that has a protected resource that is accessible by the client;

code to present at least some of the information from the session token to the second system; and

code to input, from the second system to the first system, a determination whether the client has a valid session credential granted by the second system; and

code to grant access to the protected resource on the first system, to the client based on the determination from the second system that the client has a valid session credential with the second system..

12. (previously presented) A programmed computer for validating credentials, comprising:

a memory having at least one region for storing computer executable program code; and

a processor for executing the program code stored in the memory, wherein the program code comprises:

code to input, at a first system that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first system;

code to determine, at the first system that the client does not have a valid session credential granted by the first system;

code to retrieve, at the first system, information from a session token held by the client, the information corresponding to a session credential for the second system that grants session credentials based on successful authentication at the second system, the second system including a protected resource that is accessible by the client;

code to present at least some of the information from the session token to the second system; and

code to input, from the second system to the first system, a determination whether the client has a valid session credential granted by the second system and code to grant access to the protected resource on the first system, to the client based on the determination from the second system that the client has a valid session credential with the second system.

13. (previously presented) A method for establishing session credentials comprising:

inputting, at a first system that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first system;

determining at the first system that the client does not have a valid session credential

granted by a first system;

determining that the client does not have a valid session credential granted by a second system based on successful authentication at the second system;

sending, from the first system to the client, a log in page;

receiving, at the first system from the client, log in information;

sending, from the first system to the second system, the log in information; and

receiving, at the first system from the second system, information corresponding to a session credential granted by the second system, the session credential granted by the second system based at least in part on the log in information and successful authentication at the second system, the second system being one that (1) grants session credentials based on successful authentication at the second system, and (2) includes a protected resource on the second system that is accessible by the client; and

the first system granting access, to a protected resource on the first system, to the client based on the determination from the second system that the client has a valid session credential with the second system.

14. (previously presented) A method according to claim 13, further comprising granting a session credential for the first system.

15. (previously presented) A method according to claim 13, further comprising granting a session credential for the second system.

16. (previously presented) A method according to claim 13, further comprising associating session credentials for the first system and the second system with the client.

17. (previously presented) A method for establishing session credentials for a client, the method comprising:

inputting, at a first system that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first system;

determining that the client does not have a valid session credential granted by the first system;

inputting information at the first system, from the second system, that the client does not have a valid session credential granted by the second system, the second system including a protected resource;

sending, from the second system to the client, a log in page;

receiving, at the second system from the client, log in information; and

sending, from the second system to the first system, information corresponding to a session credential granted by the second system, the session credential granted by the second system based at least in part on the log in information and successful authentication at the second system; and

granting a session credential to the client for the first system, such that the client is granted access to a protected resource on the first system.

18. (original) A method according to claim 17, further comprising granting a session credential for the second system.

19. (original) A method according to claim 17, further comprising associating session credentials for the first system and the second system with the client.

20. (previously presented) A method for validating credentials comprising:

inputting, at a first system that grants session credentials based on successful authentication, a request from a client to access a protected resource on the first system

determining, at the first system that a client does not have a valid session credential granted by the first system;

redirecting the client to the second system that grants session credentials based on successful authentication at the second system, the second system having a protected resource that is accessible by the client;

sending, from the second system to the first system, session credentials granted by the second system;

sending, from the first system to the second system, the session credentials granted by the second system;

determining, at the second system, that the session credentials granted by the second system, and received from the first system, are valid; and

sending, from the second system to the first system, information indicating that the session credentials granted by the second system are valid.

21. (original) A method according to claim 20, further comprising granting the client session credentials for the first system.

22. (Canceled)